

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-175224
(P2002-175224A)

(43) 公開日 平成14年6月21日 (2002.6.21)

(51) IntCl ⁷	識別記号	F I	テームコード* (参考)
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 B 0 8 9
H 0 4 L 12/46		H 0 4 L 12/46	E 5 K 0 3 0
12/66		12/66	B 5 K 0 3 3

審査請求 有 請求項の数 7 O L (全 6 頁)

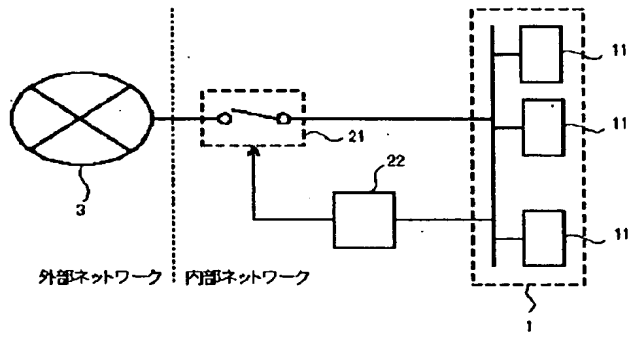
(21) 出願番号	特願2000-371240 (P2000-371240)	(71) 出願人	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22) 出願日	平成12年12月6日 (2000.12.6)	(72) 発明者	白川 洋一 東京都港区芝五丁目7番1号 日本電気株式会社内
		(74) 代理人	100095407 弁理士 木村 満
		Fターム (参考)	5B089 GA31 HA06 KA17 KB13 KC52 KC54 KG10 5K030 GA15 HA08 HC01 HC14 HD03 HD06 KA13 LB03 LC16 LD20 5K033 AA08 BA17 CB03 CB08 DA01 DA06 DB03 DB18 DB20 EA07

(54) 【発明の名称】 ネットワーク接続システム、及び装置

(57) 【要約】

【課題】 内部ネットワークに接続された計算機に対して、外部ネットワークからの不正なアクセスを防ぐと共に、内部ネットワーク内でのデータのやりとりを効率的に行う。

【解決手段】 狭い意味での内部ネットワークとしてのLAN1と、外部ネットワークとしてのWAN3との間に、回線スイッチ部21が設けられている。回線スイッチ部21は、制御部22の制御によって接続状態と切断状態とが切り替えられ、切断状態となると、WAN3からLAN1内の計算機11へのアクセスが不可能となる。回線スイッチ部21が切断状態となった場合においても、LAN1内の各計算機11同士は、接続状態にあり、自由にデータのやりとりを行うことができる。



【特許請求の範囲】

【請求項1】複数の計算機を有する内部ネットワークと、該内部ネットワークを外部ネットワークに接続するためのネットワーク接続装置を備えるネットワーク接続システムであって、

前記ネットワーク接続装置は、

一端が前記内部ネットワークに、他端が前記外部ネットワークに接続され、前記内部ネットワークと前記外部ネットワークとを実質的な接続状態と実質的な切断状態とのいずれかに切り替えるスイッチ手段と、

所定の条件が成立することによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替える制御手段とを備えることを特徴とするネットワーク接続システム。

【請求項2】前記内部ネットワークと前記外部ネットワークとの間に、前記外部ネットワークから前記内部ネットワークへのアクセスをチェックし、該アクセスが不正アクセスである場合に内部ネットワークへのアクセスを制限するファイアウォールをさらに備えることを特徴とする請求項1に記載のネットワーク接続システム。

【請求項3】前記内部ネットワークと前記外部ネットワークとは、前記外部ネットワークから前記内部ネットワークへの不正アクセスがあった場合にアラームを発生するアラーム発生手段を含むファイアウォールを介して接続されており、

前記ネットワーク接続装置は、前記ファイアウォール内の機能として実現されており、

前記制御手段は、前記アラーム発生手段がアラームを発生した場合に、前記スイッチ手段を実質的な切断状態とすることを特徴とする請求項1に記載のネットワーク接続システム。

【請求項4】複数の計算機を有する内部ネットワークを、外部ネットワークに接続するためのネットワーク接続装置であって、

一端が前記内部ネットワークに、他端が前記外部ネットワークに接続され、前記内部ネットワークと前記外部ネットワークとを実質的な接続状態と実質的な切断状態とのいずれかに切り替えるスイッチ手段と、

所定の条件が成立することによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替える制御手段とを備えることを特徴とするネットワーク接続装置。

【請求項5】前記スイッチ手段及び前記制御手段は、それぞれ前記外部ネットワークから前記内部ネットワークへの不正アクセスがあった場合にアラームを発生するアラーム発生手段を含むファイアウォールの機能として実現されており、

前記制御手段は、前記アラーム発生手段がアラームを発生した場合に、前記スイッチ手段を実質的な切断状態とすることを特徴とする請求項4に記載のネットワーク接

続装置。

【請求項6】前記制御手段は、前記内部ネットワークにおける所定の事象の発生を監視し、該所定の事象の発生によって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替えることを特徴とする請求項4または5に記載のネットワーク接続装置。

【請求項7】前記制御手段は、計時手段によって計時された時間が所定の時間となることによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替えることを特徴とする請求項4乃至6のいずれか1項に記載のネットワーク接続装置。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、LAN (Local Area Network) などの内部ネットワークと、WAN (Wide Area Network) などの外部ネットワークとを接続するネットワーク接続システム及び装置に関する。

【0002】

【従来の技術】近年、多くの計算機が何らかの形でネットワーク接続されて使用されるようになってきているが、各計算機への不正アクセスを如何にして防ぐかが大きな課題となっている。特にLANなどの内部ネットワークと、インターネットを始めとするWANなどの外部ネットワークとが接続されているネットワークシステムでは、一般に、内部ネットワークと外部ネットワークとの間にファイアウォールを設け、ファイアウォールによる認証やフィルタリングによって、各計算機が外部ネットワークから不正にアクセスされるのを防いでいる。

【0003】ところが、ファイアウォールを介したネットワーク接続システムでも、内部ネットワークに接続された各計算機は、基本的には外部ネットワークとも常時接続されていることとなる。このため、外部ネットワークからの不正アクセスを完全に遮断するのは不可能であった。そこで、各計算機において外部からの不正アクセスを防止するための技術として、特開2000-10887号公報においてセキュリティスイッチ付きネットワークインタフェースモジュールが提案されている。

【0004】図4は、特開2000-10887号公報に記載のセキュリティスイッチ付きネットワークインタフェースモジュールを示すブロック図である。図示するように、ネットワークインタフェースモジュール101は、計算機105に1対1で対応して設けられるものであり、ネットワークインタフェース102と、セキュリティスイッチ104を含む電源インタフェース103とから構成されている。

【0005】ネットワークインタフェースモジュール101の電力は、計算機105内の電源107から供給されている。CPU106が電源107からの電力の供給を停止すると、セキュリティスイッチ104がオフし、ネットワークインタフェース102が動作不能となる。

これにより、外側のネットワークから計算機105にアクセスすることが不可能になり、計算機105への不正アクセスを防ぐことができるようになっている。

【0006】

【発明が解決しようとする課題】しかしながら、特開2000-10887号公報に記載の技術では、ネットワークインタフェースモジュール101をそれぞれの計算機105に対応して設けなければならない。ところが、内部ネットワークと、外部ネットワークとが接続されたシステムでは、内部ネットワークからの計算機105への不正アクセスはあまり考えられない。このようなほとんど考えられないような不正アクセスに対して、計算機105の各々に冗長構成をするというのは、スペース及びコストの面から無駄である。

【0007】また、内部ネットワークと、さらに外部ネットワークに接続された計算機にあっては、通常、内部ネットワーク内でのデータのやりとりは頻繁に行われるが、これに対して外部ネットワークとのデータのやりとりは圧倒的に少ない。このため、特開2000-10887号公報のように計算機105の各々に対してネットワークインタフェースモジュール101を設け、計算機105の各々がアクセス拒否できるようにすると、内部ネットワーク内のみでのデータのやりとりには支障が生じてしまう可能性がある。

【0008】本発明は、内部ネットワークに接続された計算機に対して、外部ネットワークからの不正なアクセスを防ぐと共に、内部ネットワーク内でのデータのやりとりを効率的に行い得るネットワークアクセスシステム等を提供することを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するため、本発明の第1の観点にかかるネットワーク接続システムは、複数の計算機を有する内部ネットワークと、該内部ネットワークを外部ネットワークに接続するためのネットワーク接続装置を備えるネットワーク接続システムであって、前記ネットワーク接続装置は、一端が前記内部ネットワークに、他端が前記外部ネットワークに接続され、前記内部ネットワークと前記外部ネットワークとを実質的な接続状態と実質的な切断状態とのいずれかに切り替えるスイッチ手段と、所定の条件が成立することによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替える制御手段とを備えることを特徴とする。

【0010】上記のネットワーク接続システムでは、制御手段がスイッチ手段を実質的な切断状態とすることによって、外部ネットワークから内部ネットワークへのアクセスが不能となる。これにより、外部ネットワークから内部ネットワークへの不正アクセスを遮断することが可能となる。ここで、スイッチ手段が実質的な切断状態となっている場合でも、内部ネットワーク内の計算機同

士は、互いに接続状態を保ったままであり、内部ネットワーク内でのデータのやりとりには支障が生じることはない。

【0011】上記ネットワーク接続システムは、前記内部ネットワークと前記外部ネットワークとの間に、前記外部ネットワークから前記内部ネットワークへのアクセスをチェックし、該アクセスが不正アクセスである場合に内部ネットワークへのアクセスを制限するファイアウォールをさらに備えるものとすることができる。

【0012】上記ネットワーク接続システムにおいて、前記内部ネットワークと前記外部ネットワークとは、前記外部ネットワークから前記内部ネットワークへの不正アクセスがあった場合にアラームを発生するアラーム発生手段を含むファイアウォールを介して接続されたものであってもよい。この場合において、前記ネットワーク接続装置は、前記ファイアウォール内の機能として実現されたものとすることができ、前記制御手段は、前記アラーム発生手段がアラームを発生した場合に、前記スイッチ手段を実質的な切断状態とすることができる。

【0013】これら示したように、スイッチ手段に加えてファイアウォールを併用することによって、外部ネットワークから内部ネットワークへの不正アクセスをより強固に防止することができ、さらにセキュリティの高いシステムを構築することが可能となる。

【0014】上記目的を達成するため、本発明の第2の観点にかかるネットワーク接続装置は、複数の計算機を有する内部ネットワークを、外部ネットワークに接続するためのネットワーク接続装置であって、一端が前記内部ネットワークに、他端が前記外部ネットワークに接続され、前記内部ネットワークと前記外部ネットワークとを実質的な接続状態と実質的な切断状態とのいずれかに切り替えるスイッチ手段と、所定の条件が成立することによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替える制御手段とを備えることを特徴とする。

【0015】上記ネットワーク接続装置において、前記スイッチ手段及び前記制御手段は、それぞれ前記外部ネットワークから前記内部ネットワークへの不正アクセスがあった場合にアラームを発生するアラーム発生手段を含むファイアウォールの機能として実現されたものであってもよい。この場合において、前記制御手段は、前記アラーム発生手段がアラームを発生した場合に、前記スイッチ手段を実質的な切断状態とすることができる。

【0016】上記ネットワーク接続装置において、前記制御手段は、また、前記内部ネットワークにおける所定の事象の発生を監視し、該所定の事象の発生によって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替えるものとしてもできる。

【0017】上記ネットワーク接続装置において、前記

制御手段は、さらに、計時手段によって計時された時間が所定の時間となることによって、前記スイッチ手段を実質的な接続状態とするか実質的な切断状態とするかを切り替えるものとすることもできる。

【0018】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態について説明する。

【0019】図1は、この実施の形態にかかるネットワーク接続システムの構成を示すブロック図である。図示するように、このネットワーク接続システムでは、内部ネットワークとしてのLAN1に、複数の計算機11が接続されている。LAN1は、回線スイッチ部21と、制御部22とに接続されている。回線スイッチ部21及び制御部22は、広い意味での内部ネットワークに含まれる。回線スイッチ部21の他端は、外部ネットワークとしてのWAN3に接続されている。なお、具体的に述べると、LAN1はイントラネット、WAN3はインターネットとすることができる。

【0020】回線スイッチ部21は、制御部22から送られた制御信号に基づいて、LAN1とWAN3との間を接続状態とするか、切断状態とするかを切り替える。制御部22は、LAN1から得られる制御信号に基づいて、回線スイッチ部21の状態を切り替える制御信号を生成し、出力する。

【0021】制御部22は、例えば、LAN1に接続する回線ボードと、回線スイッチ部21を制御するパーソナルコンピュータ等で実現することができる。この場合、回線スイッチ部21は、シリアル信号によってLAN1とWAN3とを物理的にON/OFFするケーブルスイッチであってもよい。また、回線スイッチ部21と制御部22は、専用のハードウェア装置で実現してもよい。この場合、LAN1に接続するインタフェースとWAN3に接続されるインタフェースとが提供されていればよいこととなる。

【0022】以下、このネットワーク接続システムにおける動作について説明する。ここで、通常の状態では、回線スイッチ部21は切断状態になっているものとする。

【0023】LAN1をWAN3と接続すべき事象、例えば、計算機11のいずれかがWAN3上のコンピュータ装置にアクセスし、データを取得しようとする事象が発生したときに、当該計算機11は、制御部22にWAN3にアクセスしようとする旨を通知する。この通知に基づいて、制御部22は、回線スイッチ部21に制御信号を送り、回線スイッチ部21を接続状態に切り替えさせる。

【0024】回線スイッチ部21が接続状態となった後、当該計算機11は、WAN3上のコンピュータ装置にアクセスし、そこからデータを取得する。データの取得が終了すると、当該計算機11は、制御部22にWA

N3へのアクセスを終了した旨を通知する。この通知に基づいて、制御部22は、回線スイッチ部21に制御信号を送り、回線スイッチ部21を切断状態に切り替えさせる。

【0025】一方、WAN3上のコンピュータ装置がLAN1内の計算機11のいずれかにアクセスしようとしたとき、通常、回線スイッチ部21は切断状態となっているので、実際には計算機11にアクセスすることができない。この状態においても、LAN1内の計算機11同士は接続状態となっているため、互いに自由にデータをやりとりすることができる。

【0026】以上説明したように、この実施の形態にかかるネットワーク接続システムでは、制御部22が回線スイッチ部21を切断状態としていれば、WAN3からLAN1内の計算機11にアクセスすることができない。このため、LAN1内の計算機11が外部ネットワークとしてのWAN3とデータをやりとりの必要がない場合は、回線スイッチ部21を全て切断状態としておけばよいので、WAN3からLAN1内の計算機11に不正にアクセスされるのを防ぐことができる。

【0027】また、回線スイッチ部21が切断状態にある場合でも、LAN1内の計算機11同士は、常に接続状態を保つことができている。このため、LAN1内における計算機11同士のデータのやりとりに支障が生じることなく、LAN1内における処理を効率的に行うことができる。

【0028】本発明は、上記の実施の形態に限られず、種々の変形、応用が可能である。以下、本発明に適用可能な上記の実施の形態の変形態様について説明する。

【0029】上記の実施の形態では、制御部22は、内部ネットワークであるLAN1内において発生した事象に基づいて、回線スイッチ部21を接続状態と切断状態のいずれかに切り替えていた。これに対して、外部ネットワークであるWAN3において発生した事象によっても、回線スイッチ部21を切り替えることは可能である。もっとも、WAN3において発生した事象は、回線スイッチ部21が接続状態にある場合しか制御部22に伝えられないが、制御部22は、WAN3において発生した事象に基づいて回線スイッチ部21を適切なタイミングで接続状態から切断状態に切り替えることができる。

【0030】また、制御部22による回線スイッチ部21の接続状態と切断状態との切り替えは、タイマが計時する時間によって行うことも可能である。例えば、定期的なアプリケーションや、メールやニュースの配送、ファイルの転送やバックアップ等は、必ずしも常時接続しなければ行い得ないものではない。そこで、タイマが計時する時間に従って、予め定められた時間帯で回線スイッチ部21を接続状態とし、このようなデータの授受を行うものとすればよい。なお、タイマは、制御部22自

体が備えるものとしても、制御部22の外側にあり、時間情報を制御部22に入力可能にしたもののいずれであってもよい。

【0031】上記の実施の形態では、LAN1とWAN3とは、回線スイッチ部21を介してのみ接続されるものとしていた。これに対して、LAN1とWAN3との接続に、ファイアウォールを併用した構成のネットワーク接続システムも構成することが可能である。

【0032】図2は、ファイアウォールを併用した、他の構成のネットワーク接続システムの構成を示すブロック図である。このネットワーク接続システムでは、回線スイッチ部21とLAN1との間に、さらにファイアウォール23が設けられている。もっとも、ファイアウォール23の位置は、回線スイッチ部21とWAN3との間であってもよい。

【0033】図2のネットワークシステムにおいて、WAN3からLAN1内の計算機11に不正アクセスがあったとする。ここで、回線スイッチ部21が接続状態になっていると、その不正アクセスは、ファイアウォール23にまで達する。次に、ファイアウォール23は、WAN3からのアクセスをフィルタにかけるが、不正アクセスであるために、LAN1内の計算機11に伝えない。このような構成により、WAN3からLAN1内の計算機11への不正アクセスの防止が強化され、上記の実施の形態で示したシステムよりも、一層セキュリティの高いシステムを構築することができる。

【0034】図3は、ファイアウォールを併用した、さらに他の構成のネットワーク接続システムの構成を示すブロック図である。このネットワーク接続システムでは、LAN1とWAN3とはファイアウォール2を介して接続されており、回線スイッチ部21及び制御部22は、ファイアウォール2の機能として実現されている。ファイアウォール2は、WAN3からLAN1内の計算機11に不正アクセスがあった場合に、アラームを発するアラーム発生部24を含んでいる。

【0035】ここで、制御部22は、アラーム発生部24がアラームを発生したとき、LAN1とWAN3とが切断状態となるように、回線スイッチ部21に制御信号を送る。回線スイッチ部21が切断状態に切り替えられた後、例えば、LAN1内の計算機11からWAN3へのアクセスがあった場合に、制御部22は、再び接続状態となるよう回線スイッチ部21に制御信号を送ることができる。なお、制御部22は、アラーム発生部24がアラームを発生した場合の他に、上記したような種々の

事象が発生したときにも、回線スイッチ部21を切断状態に切り替えるように制御することができる。

【0036】このような構成としたことで、WAN3からLAN1内の計算機11へ不正なアクセスがあった場合には、ファイアウォール2としてその不正アクセスを伝えただけでなく、回線スイッチ部21も切断状態とされるので、不正アクセスの防止をより強化することができる。これにより、上記の実施の形態で示したシステムよりも、一層セキュリティの高いシステムを構築することができる。

【0037】上記の実施の形態では、LAN1を内部ネットワークとし、これに外部ネットワークとしてのWAN3が接続されたネットワーク接続システムを例として説明した。しかしながら、例えば、LANとLANとをルータなどにより接続したネットワークシステムにおいても、そのうちのいずれか1以上のLANにおいて、上記した回線スイッチ部21と制御部22とを設けることができる。

【0038】

【発明の効果】以上説明したように、本発明によれば、内部ネットワークに接続された各計算機に対して、外部ネットワークからの不正なアクセスを防止できると共に、内部ネットワーク内でのデータのやりとりを支障なく行うことができる。

【図面の簡単な説明】

【図1】本発明の実施の形態にかかるネットワーク接続システムの構成を示すブロック図である。

【図2】本発明の他の実施の形態にかかるネットワーク接続システムの構成を示すブロック図である。

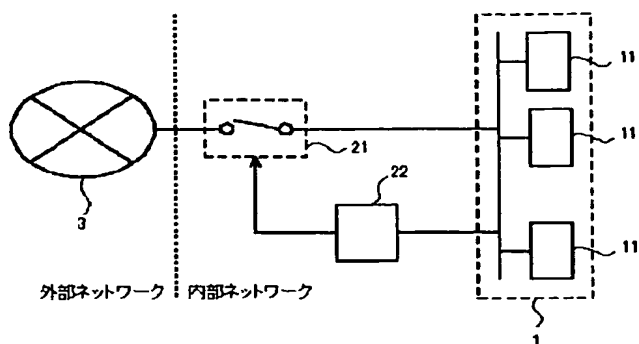
【図3】本発明の他の実施の形態にかかるネットワーク接続システムの構成を示すブロック図である。

【図4】従来例にかかるセキュリティスイッチ付きネットワークインタフェースモジュールを示すブロック図である。

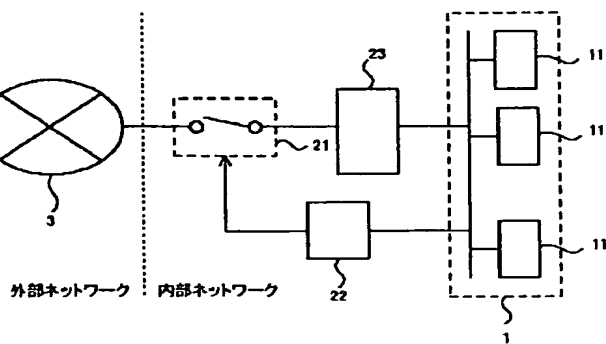
【符号の説明】

- 1 LAN
- 2 ファイアウォール
- 3 WAN
- 11 計算機
- 21 回線スイッチ部
- 22 制御部
- 23 ファイアウォール
- 24 アラーム発生部

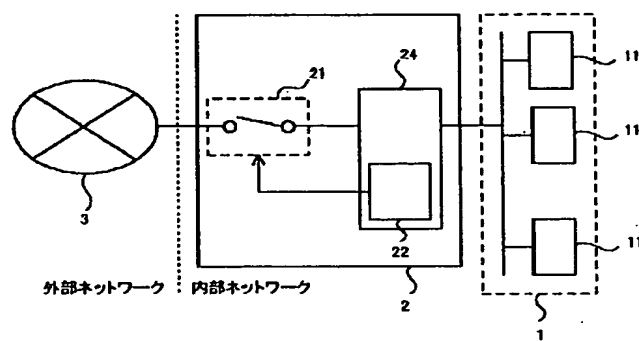
【図1】



【図2】



【図3】



【図4】

